David A. Bateman, WSBA #14262
K&L GATES LLP
925 Fourth Avenue, Suite 2900
Seattle, Washington 98104-1158
(206) 623-7580
david.bateman@klgates.com

Emily Johnson Henn
Matthew D. Kellogg
COVINGTON & BURLING LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, California 94065-1418
(650) 632-4700
ehenn@cov.com
mkellogg@cov.com

Tom Burt
MICROSOFT CORPORATION
One Microsoft Way
Redmond, Washington 98052-7329

Attorneys for Plaintiff
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, Plaintiff, v. SICHUAN CHANGHONG ELECTRIC COMPANY, LTD., Defendants.	Civil Case No.: COMPLAINT FOR INJUNCTIVE RELIEF AND DAMAGES JURY TRIAL DEMANDED

Plaintiff Microsoft Corporation ("Microsoft") brings this action against Defendant Sichuan Changhong Electric Company, Ltd. ("Changhong") to enjoin and seek damages for Changhong's continuing unauthorized access to Microsoft's servers and use of stolen product activation keys in a scheme to use unlicensed copies of Microsoft software products, and alleges as follows:

PARTIES

1. Plaintiff Microsoft is a Washington corporation with its principal place of business in Redmond, Washington.

2. Defendant Changhong is a China-based manufacturer of household electronics and appliances, including televisions, DVD players, air conditioners, batteries, and related products. Changhong is incorporated in China and is listed on the Shanghai stock exchange, with its principal place of business at 35 East Mianxing Road, Hi-Tech Park, Mianyang, Sichuan Province, People's Republic of China. Changhong is registered with the California Secretary of State and has designated Xiangtao Wu as its agent for service of process, located at 20651 Golden Springs Drive #280, Diamond Bar, California 91789.

3. Upon information and belief, Changhong has operated in the United States through three subsidiaries located in California: Changhong America Inc., with its principal place of business at 17870 Castleton Street #116, City of Industry, California 91748; Changhong International Group Inc., with its principal place of business at 7824 Balboa Boulevard, Van Nuys, California 91406; and Changhong Trading Corp., USA, with its principal place of business at 2311 East Locust Court, Ontario, California 91761.

JURISDICTION AND VENUE

4. This action arises out of Changhong's violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Microsoft seeks damages and injunctive relief to remedy Changhong's use of stolen product activation keys to gain unauthorized access to Microsoft's servers, which are protected computers under 18 U.S.C. § 1030(e)(2)(B), through which Changhong also exceeded authorized access to Microsoft's servers by obtaining information that Changhong was not authorized to obtain and which Changhong used to activate Microsoft software that Changhong was not authorized to install or activate.

5. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 and 18 U.S.C. § 1030, in that the cause of action arises under the laws of the United States.

6. This Court has personal jurisdiction over Changhong because Changhong purposefully availed itself of the privilege of conducting activities in this forum or purposefully directed its activities towards this forum, causing harm to Microsoft that Changhong knew would affect Microsoft in this forum; Microsoft's claims arise from Changhong's forum-related activities; and the exercise of personal jurisdiction over Changhong is reasonable. Upon information and belief, Changhong has long known that Microsoft owns both the software that Changhong activated and the activation servers that Changhong illegally accessed, and that Microsoft and its activation servers are located in Washington State.

7. Venue in this District is proper under 28 U.S.C. § 1391(b), in that a substantial part of the events or omissions giving rise to the claims pled herein occurred in the Western District of Washington and/or a substantial part of the property that is the subject of the action is situated in this District.

THE PRESENT CONTROVERSY

The Global Problem of Software Theft

8. U.S. software developers lose more than $60 billion in revenue annually from software theft—the unauthorized and unlawful copying, downloading, sharing, or selling of their copyrighted software. *See* BUSINESS SOFTWARE ALLIANCE ("BSA"), SHADOW MARKET: 2011 BSA GLOBAL SOFTWARE PIRACY STUDY 2 (2012), http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf. These losses hinder the ability of U.S. software developers like Microsoft to hire and retain employees, develop new products, and invest in future innovations.

9. Microsoft develops and sells software products for personal computers ("PCs"), servers, and other computing devices. These products include, among others, Windows 7, a widely used PC operating system, and Office 2010 and Office 2013, suites of productivity applications used for word processing, creating and editing spreadsheets, and other common tasks. Microsoft's software products are purchased not just by individuals for

their personal use, but also by companies, organizations, and other entities for business-oriented, multi-user (or "enterprise") environments.

10. Companies that develop software are not the only victims of enterprise software theft. Businesses that pay for their software are placed at an unfair disadvantage in the marketplace when forced to compete against enterprises using stolen software, as their input costs are correspondingly higher. In response, several states recently have taken action to address this unlawful market distortion and protect law-abiding businesses by enforcing those states' unfair competition laws against enterprises that use stolen software. *See, e.g.*, CALIFORNIA DEPT. OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL, *Attorney General Kamala D. Harris Files Unfair Competition Lawsuits over Use of Pirated Software in Apparel Industry*, Jan. 24, 2013, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-unfair-competition-lawsuits-over-use; OFFICE OF ATTORNEY GENERAL OF MASSACHUSETTS, *Company Fined for Using Pirated Software to Gain Unfair Advantage Over Massachusetts Businesses*, Oct. 18, 2012, http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-10-18-narong-seafood-co.html.

11. The use of stolen software by enterprises also poses risks to Internet security. Experts have noted that stolen software has a relatively greater risk of being infected with, or vulnerable to, malicious software, commonly known as "malware." *See* FEDERAL BUREAU OF INVESTIGATION ("FBI"), *Consumer Alert: Pirated Software May Contain Malware*, Aug. 1, 2013, http://www.fbi.gov/news/stories/2013/august/pirated-software-may-contain-malware/. Once installed on a computer, malware can record a user's keystrokes, thereby capturing sensitive information such as user names, passwords, and personally identifiable information like Social Security numbers and birthdates. *Id.* Malware also can be exploited by malicious actors to create "botnets"—vast networks of malware-infected computers that are controlled remotely to perform criminal acts such as attacking corporate networks and perpetuating fraud. *See* FBI, *FBI Statement on Botnet Operation*, June 5, 2013, http://www.fbi.gov/news/news_blog/botnets-101/fbi-statement-on-botnet-operation (announcing disruption of more

than 1,000 botnets used to commit an estimated $500 million or more in financial fraud). Accordingly, software theft may increase security risks for Internet users broadly, not just for users of stolen software.

12. While software theft exists everywhere in the world, it is especially pervasive in emerging markets such as China, Brazil, and India. The BSA estimated a 68 percent rate of software theft in emerging markets in 2011, meaning that more than two of every three copies of software used in those markets was stolen. 2011 BSA GLOBAL SOFTWARE PIRACY REPORT, *supra*, at 6. In China, the rate was even higher, reaching 77 percent. *Id.* By comparison, the rate of software theft across mature markets during the same period was 24 percent, with a U.S. rate of 19 percent. *Id.*

13. One reason that software theft is more common in some emerging markets is the difficulty of effectively enforcing intellectual property and other rights in software under local legal systems. Attempting to combat software theft in many emerging markets can be expensive and result in little or no compensation to owners of the stolen software. As a result, in-country enforcement actions to combat enterprise software theft often do little to deter other organizations from engaging in such theft. Despite the fact that nearly every country in the world has passed legislation to protect copyrights in software, inadequate remedies for theft and the unavailability of effective judicial process in certain countries mean that in-country enforcement actions often are ineffective.

Countering Software Theft Through Cyberforensics

14. Like many other software developers, Microsoft has undertaken a wide range of initiatives to protect customers and combat theft of its products. These efforts include educating users about the risks of using stolen software, engineering Microsoft products and packaging to help users identify genuine products and distinguish them from stolen products, and investigating and pursuing actions against infringers as well as assisting efforts by law enforcement to tackle cybercrime. In support of these initiatives, Microsoft recently launched its Cybercrime Center to combat software theft and other digital crimes such as online fraud

and identity crimes. Among other tools, the Cybercrime Center uses cyberforensics, a new investigative technique that relies on state-of-the-art technology to detect and identify attempts to gain unauthorized access to Microsoft's systems.

15. One important component of cyberforensics is Microsoft's product activation system, a technology in which Microsoft has invested heavily. One of the goals of product activation is to reduce theft of Microsoft products and help ensure that Microsoft's legitimate customers receive the product quality they expect. Over time, reducing software theft will enable Microsoft to invest more resources into product development, quality control, and support, ensuring better products and more innovation for customers.

16. Enterprise customers typically purchase copies of Microsoft software products through volume licensing. When purchasing Microsoft software through volume licensing, an enterprise customer typically purchases a specified number of licenses. An enterprise customer is authorized to install copies of the software on its computers in accordance with the number of licenses it purchased. The number of licenses purchased, along with the licensing terms for these software products, are set forth in the volume-licensing agreement or other agreements between Microsoft and the enterprise customer. Only by purchasing or otherwise lawfully obtaining a license for a Microsoft software product is a user authorized by Microsoft to install and use that product.

17. Product activation, which applies to certain Microsoft products, is the process whereby a user is prompted to enter a Microsoft product activation key—a unique combination of numbers and letters—to "activate" the Microsoft software product. The activation process is analogous to activating credit cards or mobile phones with a code provided by the financial institution or mobile service provider. As with activation of credit cards and mobile phones, a principal purpose of Microsoft's product activation system is to identify and prevent fraud and theft—in this case, to help prevent the unlawful installation or use of Microsoft software products.

18. When an enterprise customer enters into a volume-licensing agreement with Microsoft, Microsoft assigns the customer a product activation key, which that customer is then authorized to use to activate each licensed copy of Microsoft software that it has purchased. Each key is assigned to a particular customer and is subject to limitations set forth in the licensing and other agreements associated with that key. Microsoft's licenses and associated customer agreements state that the key is solely for the use of that customer and that the customer should not disclose the product activation key to third parties. The use of a volume-licensing product activation key by anyone other than the specific customer to which the key was assigned is prohibited. Therefore, an enterprise that activates Microsoft software using a product activation key that was assigned to a different user is using that product activation key without authorization.

Accessing Microsoft Servers During Product Activation

19. In certain situations, in order to activate a copy of Microsoft software, a user (for example, an employee of an enterprise customer) must contact Microsoft over the Internet or by phone. Most enterprise customers elect to activate software over the Internet. When this occurs, the user prompts his or her computer to connect to and access Microsoft's servers, and in most cases, the user's computer contacts Microsoft's servers in Washington State, which are connected to the Internet. Microsoft then determines whether the product activation key provided by the user is valid. If it is, Microsoft's activation servers respond by sending a confirmation code to the user's computer permitting the software to complete activation. Otherwise, Microsoft's activation servers return an error code, which instructs the copy of Microsoft software not to complete activation.

User Benefits of Software Activation

20. During the activation process, a user is typically prompted to enter the product activation key that Microsoft has assigned to that user. If the user does not enter a product activation key, pop-ups and desktop notifications regularly alert the user that the product must be activated and that the user's assigned product activation key is required to do so. These

warnings continue until the software is activated. Furthermore, with respect to some versions of Microsoft software, if the user fails to activate the product within a certain period after installation (*e.g.*, 30 days), the user will experience reduced software functionality. Avoiding reduced functionality is a substantial benefit of the activation process.

21. Activating a copy of Microsoft software has additional benefits. For example, users who fail to complete installation of their software through product activation may be ineligible for certain software updates as well as for certain customer support services. Users thus obtain significant value from successfully activating their software.

Theft and Unauthorized Use of Product Activation Keys

22. Some organizations try to obtain the benefits of activated Microsoft software illegally, without purchasing a license. To do so, these enterprises typically acquire stolen product activation keys from cybercriminals who steal such keys through a number of unlawful means. For example, some cybercriminals may use social engineering techniques to obtain product activation keys that have been assigned to, or that are intended for the use of, existing Microsoft customers. Cybercriminals also may fraudulently subscribe—sometimes using stolen credit cards—to one or more of Microsoft's software subscription programs intended to benefit students, educators, and academic institutions, and steal valid product activation keys through these services. Once stolen, these keys are then sold or otherwise illegally distributed through a number of channels including online marketplaces, blogs, forums, and other Internet sites. It is through these channels that organizations seeking to activate stolen copies of Microsoft software may gain access to stolen product activation keys.

23. Upon determining that a product activation key has been stolen, Microsoft typically blocks that key so that it can no longer be used by anyone—even its original assignee—to activate Microsoft software. Accordingly, when a product activation key is blocked, the legitimate Microsoft customer to whom the key was assigned typically must deploy a new product activation key. This disruptive, costly, and time-consuming process is a

direct consequence of the theft and use of product activation keys by unauthorized organizations.

Changhong's Unauthorized Access to Microsoft Servers

24. Based on a forensic analysis of unauthorized software activations, Microsoft determined that Changhong, its employees, contractors, or other agents repeatedly activated or attempted to activate Microsoft software products using product activation keys that were stolen from licensed Microsoft customers. Changhong's use of stolen product activation keys to activate unlicensed copies of Microsoft software on Changhong computers resulted in Changhong, its employees, contractors, or other agents accessing Microsoft's activation servers without authorization. Furthermore, Changhong's use of stolen product activation keys to obtain confirmation codes from Microsoft's activation servers to which Changhong, its employees, contractors, or other agents were not entitled—and thereby to activate copies of Microsoft software that were unlicensed and therefore infringing—exceeded Changhong's authorized access to Microsoft's activation servers.

25. From on or about 2011 to the present, Changhong activated numerous copies of Microsoft software products via the Internet using stolen product activation keys. In each instance, Changhong, its employees, contractors, or other agents used stolen product activation keys to intentionally access without authorization Microsoft's activation servers located in Washington, or, in the alternative, to intentionally exceed Changhong's authorized access to those activation servers. As a result, Changhong, its employees, contractors, or other agents, acting without authorization, obtained from Microsoft's activation servers information that provided substantial value—namely, the ability to activate unlicensed copies of Microsoft software that Changhong was not authorized to activate.

26. To identify these instances of unauthorized access and access exceeding authorization, Microsoft conducted a forensic analysis of suspect activation events. Microsoft's investigation revealed numerous unauthorized activation attempts using stolen product activation keys originating from Changhong-controlled computers. These

unauthorized activation attempts resulted in Changhong's unauthorized access to Microsoft's servers, or access exceeding authorization.

27. In several of these instances, Changhong, its employees, contractors, or other agents activated or attempted to activate Microsoft software using product activation keys that had been stolen from Microsoft customers, including a U.S. public university, a U.S.-based engineering company, and a U.S. public school district. As described above, the unauthorized use of stolen product activation keys by Changhong, its employees, contractors, or other agents to access Microsoft's servers without authorization and exceeding authorized access has imposed substantial harms on both Microsoft and Microsoft's customers.

28. In several instances, Changhong, its employees, contractors, or other agents activated or attempted to activate unlicensed Microsoft software by serially entering different stolen product activation keys in rapid succession until the software successfully activated with a stolen key that Microsoft had not yet blocked. This pattern of behavior has no legitimate rationale and demonstrates that Changhong's unauthorized access to Microsoft's activation servers was intentional.

29. Microsoft's forensic analysis further revealed that the activation attempts were made from numerous devices controlled by Changhong. The activation attempts occurred frequently during regular business hours over the course of several months, with the vast majority of such attempts taking place Monday through Friday between the hours of 9:00 a.m. and 5:00 p.m. China Standard Time ("CST"). Moreover, the Microsoft software products that were the subject of the activation attempts are products routinely used for business purposes, such as the Office 2010 suite of productivity applications. Accordingly, upon information and belief, Changhong directed or encouraged its employees, contractors, or other agents to activate copies of Microsoft software using stolen product activation keys, and Changhong benefitted from such activity.

30. For example, on January 12, 2012, the user of a Changhong-controlled hardware device attempted to activate Microsoft Visio Premium 2010 using two different

stolen product activation keys in a span of three minutes until the software activated successfully. Less than an hour earlier, the user of the same device successfully activated copies of Microsoft Office Professional Plus 2010 and Microsoft Project Professional 2010, also using stolen product activation keys. The original authorized assignees of these stolen product activation keys included an Asia-based semiconductor manufacturer and a U.S. public school district. These activation attempts took place during regular business hours on a Thursday, between 3:30 p.m. and 4:30 p.m. CST.

31. Similarly, on May 10, 2013, the user of a Changhong-controlled hardware device attempted to activate Microsoft Office Professional Plus 2013 using a stolen product activation key five times in a span of twelve minutes. When those attempts failed, the user of the same device deployed a different stolen product activation key to activate the software successfully. The legitimate assignee of both stolen product activation keys was an educational institution located in China. These activation attempts took place during regular business hours on a Friday, between 4:57 p.m. and 5:14 p.m. CST.

32. In each instance, Changhong, its employees, contractors, or other agents used stolen product activation keys to intentionally access without authorization Microsoft's activation servers located in Washington, or, in the alternative, to intentionally exceed Changhong's authorized access to those activation servers. As a result, Changhong, its employees, contractors, or other agents used stolen product activation keys to obtain information without authorization from Microsoft's activation servers that enabled them to activate copies of Microsoft software that Changhong was not authorized to activate.

33. Further, while this forensic analysis enabled Microsoft to identify certain unauthorized activation attempts by Changhong, the results of the analysis likely understate significantly the overall scope and frequency of Changhong's use of stolen Microsoft software products, as such analysis focuses on certain attempts to activate software and does not capture every instance of unauthorized software use.

Value of Changhong's Unlawful Access

34. By illegally accessing Microsoft servers through the use of stolen product activation keys in order to activate unlicensed copies of Microsoft software, Changhong has obtained value to which it was not entitled.

35. First, Changhong activated copies of Microsoft software products without lawfully purchasing licenses to those copies.

36. Second, by activating Microsoft software using stolen product activation keys, Changhong illegally obtained the full benefits and functionality of the software, including giving the appearance to employees and customers that the software was licensed.

37. Third, by activating copies of Microsoft software through the use of stolen product activation keys, Changhong obtained access to software updates and support services for which only legitimate customers of Microsoft software are eligible.

Damages Caused by Changhong's Unlawful Access

38. In addition to the harm to Microsoft's customers who are the legitimate assignees of the stolen product activation keys and the associated harm to Microsoft's goodwill, this unlawful access by Changhong, its employees, contractors, and other agents has caused financial harm to Microsoft in the form of lost revenue from the software products activated without authorization as well as Microsoft's costs to investigate the unlawful access to Microsoft's servers and unauthorized use of Microsoft's software products.

COUNT I—COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030)

39. Microsoft incorporates and realleges each and every allegation contained in paragraphs 1–38 of this Complaint.

40. In engaging in the conduct described above, including, but not limited to, the use of stolen product activation keys to improperly access Microsoft's activation servers, Changhong, its employees, contractors, or other agents intentionally accessed protected computers without authorization or exceeded authorized access to protected computers and thereby obtained information from these computers that allowed them to activate Microsoft

software that Changhong was not authorized to activate. This conduct falls within the scope of 18 U.S.C. § 1030(a)(2).

41. Additionally, in accessing and directing and encouraging its employees, contractors, or other agents to access protected computers without authorization or exceeding authorized access through the use of these stolen product activation keys, Changhong acted knowingly and with intent to defraud, furthered its intended fraud through its improper access, and fraudulently obtained valuable information from Microsoft's activation servers as a result of its improper access within the scope of 18 U.S.C. § 1030(a)(4).

42. Changhong caused Microsoft damage within a one-year period in excess of $5,000 both because the value of the unlicensed software improperly activated and/or installed by Changhong far surpasses this amount and because Microsoft was forced to expend resources in excess of this amount to investigate, police, and address Changhong's unlawful activities.

43. Microsoft seeks compensatory damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

44. As a direct result of Changhong's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Changhong's actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays for judgment against Changhong as follows:

a. An award of compensatory damages as alleged above;

b. An injunction prohibiting Changhong and its employees, contractors, and other agents from obtaining stolen product activation keys for Microsoft software;

c. An injunction prohibiting Changhong and its employees, contractors, and other agents from accessing or attempting to access Microsoft's servers without Microsoft's express authorization; and

c. Such other relief at law or equity as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Microsoft hereby demands trial of its claims by jury to the full extent authorized by law.

DATED: December 17, 2013

By: /s/ David A. Bateman

David A. Bateman, WSBA #14262
K&L GATES LLP
925 Fourth Avenue, Suite 2900
Seattle, Washington 98104-1158
(206) 623-7580
david.bateman@klgates.com

Emily Johnson Henn
Matthew D. Kellogg
COVINGTON & BURLING LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, California 94065-1418
(650) 632-4700
ehenn@cov.com
mkellogg@cov.com

Tom Burt
MICROSOFT CORPORATION
One Microsoft Way
Redmond, Washington 98052-7329

Attorneys for Plaintiff
MICROSOFT CORPORATION